Algebraic Number Theory
Solutions to Example Sheet 1

3. Suppose d_1, d_2 are squarefree integers $\neq 0, 1$.
   (i) Show $\mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2})$ if and only if $d_1 = d_2$.
   (ii) Suppose $d_1 \neq d_2$ and let $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$.
   - Write down a basis for $K/\mathbb{Q}$.
   - Show that $K = \mathbb{Q}(\sqrt{d_1} + \sqrt{d_2})$.

Answer:

(i) Suppose $\mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2})$. Then $\sqrt{d_2} \in \mathbb{Q}(\sqrt{d_1})$ and so $\sqrt{d_2} = a + b\sqrt{d_1}$ where $a, b \in \mathbb{Q}$. Squaring and rearranging we obtain

$$(a^2 + b^2 d_1 - d_2) + 2ab\sqrt{d_1} = 0.$$

However 1, $\sqrt{d_1}$ are linearly independent over $\mathbb{Q}$. Thus

$$a^2 + b^2 d_1 = d_2, \qquad ab = 0.$$

If $b = 0$ then $\sqrt{d_2} = a \in \mathbb{Q}$ giving a contradiction. Hence $a = 0$. So $b^2 d_1 = d_2$. Write $b^2 = c_1^2/c_2^2$ where c_1, c_2 are coprime integers. Thus

$$c_1^2 d_1 = c_2^2 d_2.$$

Now c_1^2 must divide d_2 which is squarefree, so $c_1^2 = 1$, and similarily $c_2^2 = 1$. Hence $d_1 = d_2$.

(ii)
- Suppose $d_2 \neq d_1$. The above argument shows that $\sqrt{d_2} \notin \mathbb{Q}(\sqrt{d_1})$. Thus $\sqrt{d_2}$ has minimal polynomial $X^2 - d_2$ over $L = \mathbb{Q}(\sqrt{d_1})$. Hence a basis for K/L is 1, $\sqrt{d_2}$. We know that a basis for $L/\mathbb{Q}$ is 1, $\sqrt{d_1}$. By the tower law, a basis for $K/\mathbb{Q}$ is 1, $\sqrt{d_1}$, $\sqrt{d_2}$, $\sqrt{d_1}\sqrt{d_2}$.

- Now let $\alpha = \sqrt{d_1} + \sqrt{d_2} \in K$. Let $M = \mathbb{Q}(\alpha) \subseteq K$. If $\alpha = 0$ then $d_1 = d_2$ giving a contradiction, so $\alpha \neq 0$. Now

$$\alpha^2 - 2\sqrt{d_1}\alpha + d_1 = (\alpha - \sqrt{d_1})^2 = d_2.$$

Thus

$$\sqrt{d_1} = \frac{\alpha^2 + d_1 - d_2}{2\alpha} \in M.$$

Similarly $\sqrt{d_2} \in M$. Thus $K \subseteq M$. Hence $K = M = \mathbb{Q}(\sqrt{d_1} + \sqrt{d_2})$.

Alternative:
$\alpha^2 = d_1 + 2\sqrt{d_1 d_2} + d_2$ so $\sqrt{d_1 d_2} \in K$.
Hence $\alpha\sqrt{d_1 d_2} = d_2\sqrt{d_1} + d_1\sqrt{d_2} \in K$.
Now (d_2, d_1) is not proportional to $(1, 1)$, so we can combine this with $\sqrt{d_1} + \sqrt{d_2} \in K$ and solve linear equations to show that $\sqrt{d_1}, \sqrt{d_2} \in K$.

5. Again let p be a prime number and $\zeta_p = \exp(2\pi i/p)$. Let $K = \mathbb{Q}(\zeta_p)$ and $\alpha = 1 + \zeta_p$. Calculate $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)$ by using the minimal polynomial of α.

Answer:
From question 4, the minimal polynomial of ζ_p is $f(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$. Then $g(X) = f(X-1)$ is a monic irreducible polynomial which has $\alpha = 1 + \zeta_p$ as a root, hence $g(X)$ is the minimal polynomial of α over $\mathbb{Q}$. We can calculate $g(X) = (X-1)^{p-1} + (X-1)^{p-2} + \cdots + (X-1) + 1$. The constant coefficient is

$$a_0 = (-1)^{p-1} + (-1)^{p-2} + \cdots + (-1) + 1 = \begin{cases} 0 \text{ if } p \text{ is even,} \\ 1 \text{ if } p \text{ is odd.} \end{cases}$$

Since $K = \mathbb{Q}(\alpha)$, we have $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = (-1)^{p-1} a_0$. Thus

$$\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = \begin{cases} 0 \text{ if } p = 2, \\ 1 \text{ if } p \text{ is odd.} \end{cases}$$

6. Let $f(X) = X^3 - 2X - 2$.
   (i) Show that f is irreducible.
   (ii) Let θ be a root of f. Find the minimal polynomial for $1 + \theta + \theta^2$.

Answer:
(i) Note $f(X) = a_0 + a_1 X + a_2 X^2 + a_3 X^3$ with $a_0 = a_1 = -2$, $a_2 = 0$ and $a_3 = 1$. Let $p = 2$. Thus $p \nmid a_3$, $p \mid a_0$, $p^2 \nmid a_0$ and $p \mid a_1$, a_2. By Eisenstein's criterion with $p = 2$ the polynomial f is irreducible.

(ii) Let $\alpha = 1 + \theta + \theta^2$. We calculate matrices with respect to the basis $1, \theta, \theta^2$ for $\mathbb{Q}(\theta)$.
We have

$$m_\theta(1) = \theta, \quad m_\theta(\theta) = \theta^2, \quad m_\theta(\theta^2) = \theta^3 = 2 + 2\theta,$$
$$m_{\theta^2}(1) = \theta^2, \quad m_{\theta^2}(\theta) = 2 + 2\theta, \quad m_{\theta^2}(\theta^2) = \theta.\theta^3 = \theta(2 + 2\theta) = 2\theta + 2\theta^2$$

so

$$M_\theta = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix}, \quad M_{\theta^2} = \begin{pmatrix} 0 & 2 & 2 \\ 0 & 2 & 2 \\ 1 & 0 & 2 \end{pmatrix}.$$

Hence

$$M_\alpha = I + M_\theta + M_{\theta^2} = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 3 & 4 \\ 1 & 1 & 3 \end{pmatrix}.$$

Thus

$$\chi_{K,\alpha}(X) = \det(XI - M_\alpha) = X^3 - 7X^2 + 7X - 3.$$

Let μ be the minimal polynomial of α over $\mathbb{Q}$. Then $\chi_{K,\alpha} = \mu^n$ where $n = [K : \mathbb{Q}(\alpha)]$ which divides $[K : \mathbb{Q}] = 3$. If $n = 3$ then $\mathbb{Q}(\alpha) = \mathbb{Q}$ and so $\alpha \in \mathbb{Q}$, contradicting the fact that $1, \theta, \theta^2$ are linearly independent over $\mathbb{Q}$. Hence $\alpha \notin \mathbb{Q}$ so

$$\mu(X) = \chi_{K,\alpha}(X) = X^3 - 7X^2 + 7X - 3.$$

Alternative:
A quicker way to calculate the matrix M_α (instead of using the hint) is just to work out:

$$\begin{aligned} m_\alpha(1) &= 1 + \theta + \theta^2, \\ m_\alpha(\theta) &= \theta + \theta^2 + \theta^3 = 2 + 3\theta + \theta^2 \\ m_\alpha(\theta^2) &= 2\theta + 3\theta^2 + \theta^3 = 2 + 4\theta + 3\theta^2. \end{aligned}$$

Then you can read off M_α.

Feedback

Solutions were generally very good. The most common places to lose marks were:

Q3. When you have $b^2 d_1 = d_2$ and want to deduce that $d_1 = d_2$, it is not enough to say that d_2 is square-free, you have to use that d_1 is also square-free (because b is only a rational number, not necessarily an integer.

Q5. Many people forgot the $p = 2$ case.

Q6. You have to give some argument for why the minimal polynomial of α is equal to $\chi_{K,\alpha}$. There are a variety of ways to do this: you can show that $K = \mathbb{Q}(\alpha)$, or you can prove that $\chi_{K,\alpha}$ is irreducible (e.g. by shifting and using Eisenstein) or that it is not the cube of a polynomial (because the constant term is not a cube).